

SUPNUM

RSS

Homework

Audit de Vulnérabilités et Rédaction de Rapport

Introduction à la sécurité informatique

Mohamed Said M'Bareck
2025-2026

Objectifs du Devoir

Ce devoir vise à vous faire franchir l'étape suivante après l'énumération manuelle : l'utilisation d'un scanner de vulnérabilités professionnel. L'objectif n'est pas seulement de *trouver* des failles, mais surtout de savoir les *valider*, les *contextualiser* et les *présenter* dans un rapport d'audit cohérent.

Contexte

Le TD 2 nous a permis de découvrir manuellement des services, des versions et des failles de configuration simples. Dans un audit réel, cette démarche est complétée par des scans automatisés pour couvrir un périmètre large et identifier rapidement les vulnérabilités connues (CVEs).

Votre mission est de vous équiper d'un de ces scanners, d'auditer un sous-réseau, et de produire le livrable le plus important d'un auditeur : le **rapport de test d'intrusion**.

Tâches à Réaliser

1. Installation d'un Scanner de Vulnérabilités

Vous devez installer et configurer l'un des deux scanners de référence :

- **OpenVAS (Greenbone)** : La solution open-source de référence. L'installation peut être complexe, mais elle est très formatrice.
- **Nessus Essentials** : La version gratuite (limitée à 16 IPs) du scanner commercial le plus populaire.

Note d'installation

Pour OpenVAS, nous vous recommandons d'utiliser la **Greenbone Community Edition** via les paquets de votre distribution (Kali Linux le fournit) ou via Docker. Pour Nessus, l'enregistrement à **Nessus Essentials** est gratuit sur le site de Tenable.

2. Audit du Réseau Cible

Une fois votre scanner opérationnel, configurez un nouveau scan (un "Network Scan" basique est suffisant) et lancez-le sur le périmètre suivant :

- **Cible du Scan** : 10.10.7.0/24

Laissez le scan se terminer et exportez les résultats.

3. Validation et Analyse Critique des Résultats

C'est l'étape la plus importante. Un scanner génère beaucoup de "bruit" et de **faux positifs**. Votre travail d'analyste commence ici.

Pour chaque vulnérabilité "Critique" ou "Élevée" trouvée :

1. **Confirmez la CVE** : Recherchez sur Internet (ex : cve.mitre.org, NVD) pour comprendre la vulnérabilité. Est-elle pertinente dans le contexte du service trouvé ?
2. **Validez la Faille** : Utilisez un autre outil pour confirmer la découverte. Par exemple :
 - Si Nessus trouve un "Apache 2.4.x" obsolète, vérifiez la version avec `nmap -sV` ou `netcat`.

- Si OpenVAS signale une "Connexion anonyme FTP", essayez de vous connecter manuellement avec `ftp <IP>`.
 - Vous pouvez utiliser `searchsploit` pour voir s'il existe des exploits publics.
3. **Optionnel** : Tenter d'exploiter la vulnérabilité est un plus, mais n'est pas obligatoire pour ce devoir. La validation (confirmation qu'elle existe) est suffisante.

4. Rédaction d'un Rapport de Test d'Intrusion

Vous devez rédiger un rapport professionnel (3 à 5 pages) qui synthétise vos trouvailles. Ce rapport doit être clair, concis et aller à l'essentiel.

Structure Attendue du Rapport

Votre rapport DOIT inclure les sections suivantes :

1. **Synthèse Managériale (Management Summary)**
 - Un résumé d'un paragraphe destiné à un public non technique, expliquant le niveau de risque global et les actions prioritaires.
2. **Périmètre et Méthodologie**
 - Quel réseau a été scanné (10.10.7.0/24) ?
 - Quels outils ont été utilisés (Nessus/OpenVAS, Nmap, etc.) ?
3. **Détail des Vulnérabilités (Les 3 plus critiques)**
 - **Nom** : Ex : "Exécution de code à distance sur..."
 - **Criticité** : Ex : Élevée / 8.5 (CVSS)
 - **Description** : Qu'est-ce que la faille ?
 - **Preuve de Concept (PoC)** : Comment l'avez-vous validée ? (C'est ici que vous mettez vos captures d'écran de `nmap` ou `ftp`).
4. **Recommandations et Plan de Remédiation**
 - Que faut-il faire pour corriger chaque faille ? (Ex : "Mettre à jour le service Apache", "Désactiver l'accès anonyme FTP").

Bon courage !